IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

---

YVONNE MART FOX, GRANT NESHEIM,
DANIELLE DUCKLEY, and SHELLY KITSIS,
on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

IOWA HEALTH SYSTEM d/b/a
UNITYPOINT HEALTH,

Defendant.

OPINION and ORDER

18-cv-327-jdp

---

Defendant UnityPoint Health runs a network of hospitals, clinics, home care services, and health insurers throughout Wisconsin, Iowa, and Illinois. In 2017 and 2018, UnityPoint's email system was hacked. Plaintiffs, all customers of UnityPoint, say that hackers obtained their private health information and other personal identifying information (such as Social Security numbers) that can be used to commit identity theft. Plaintiffs filed this proposed class action, asserting 14 different claims under Wisconsin, Illinois, and Iowa law. UnityPoint moves to dismiss under Federal Rule of Civil Procedure 12(b)(1) for lack of standing and under Rule 12(b)(6) for failure to state a claim upon which relief may be granted. Dkt. 27.

The court will grant the motion only in part. Plaintiffs allegations are sufficient to establish standing under Article III of the Constitution. The court will dismiss some of plaintiffs' claims for failure to state a claim: (1) Shelly Kitsis and Danielle Duckley's claims for negligence and negligence per se because they are barred by the Illinois and Iowa economic loss doctrines; (2) plaintiffs' claims for invasion of privacy because they do not allege that UnityPoint intentionally released their information; (3) plaintiffs' common law and statutory misrepresentation claims because plaintiffs have not pleaded reliance or damages; and

(4) plaintiffs' claim under Wisconsin's data breach notification statute, Wis. Stat. § 134.98, because it does not create a private right of action. The court will also exercise its discretion to decline to hear plaintiffs' claim for declaratory relief under the Declaratory Judgment Act. Plaintiffs may proceed on all other claims. Plaintiffs ask for leave to amend their complaint to cure any deficiencies that lead to claims being dismissed. But because any amendment would likely be futile, the court will deny the request.

Also before the court is plaintiffs' notice of supplemental authority, Dkt. 51, and UnityPoint's motion for leave to respond to the supplemental authority, Dkt. 52, which plaintiffs oppose. Plaintiffs' motion is granted; UnityPoint's is denied. But the supplemental authority is a district court case from outside this jurisdiction which addresses the issue of standing in data breach cases. There is already binding authority in this jurisdiction on the issue of standing, so the supplemental authority adds little to the analysis. UnityPoint has also its own notice of supplemental authority. Dkt. 54. The court will accept UnityPoint's supplemental authority, but it too adds little to the analysis. That case is about standing to sue for violations of the Fair Credit Reporting Act. It did not involve a data breach, or any other allegations that are analogous to this case.

## ALLEGATIONS OF FACT

The court draws the following facts from plaintiffs' amended complaint. Dkt. 22.

Plaintiffs are customers of UnityPoint. Yvonne Fox and Grant Nesheim live and use UnityPoint services in Wisconsin, Danielle Duckley lives and uses UnityPoint services in Illinois, and Shelly Kitsis lives and uses UnityPoint services in Iowa.

As part of its health care and insurance business, UnityPoint stores the personal information of its patients and customers. This information includes patient names, Social Security numbers, payment information, phone numbers, and email addresses. UnityPoint also keeps patient health care information, such as lab results, treatment notes, and diagnoses. Its privacy policy promises to use security procedures to protect personal information from misuse or unauthorized disclosure. The policy says that UnityPoint will store personal information "in a secure database behind an electronic firewall." Dkt. 22, ¶ 156. In the event of a data breach, UnityPoint says it will notify customers "without unreasonable delay but in no case later than 60 days after we discover the breach." *Id.* A copy of the privacy policy was given to all UnityPoint customers.

**A. First data breach**

Around November 1, 2017, hackers gained access to UnityPoint employee email accounts and stole the personal health information of more than 16,000 UnityPoint patients. The hackers were "motivated to steal" and "specifically targeted" health information and other sensitive information like Social Security numbers. *Id.*, ¶ 24. UnityPoint discovered the data breach between February 7 and February 15, 2018, but it did not notify the public until two months later, when it sent a letter to those affected by the breach. The letter stated:

> [UnityPoint] discovered your protected health information was contained in an impacted email account, including your name and one or more of the following: date of birth, medical record number, treatment information, surgical diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information . . . The information did not include your Social Security number.

*Id.*, ¶¶ 20–21.

UnityPoint knew that this letter was not accurate. On the same day that it sent the letter, it disclosed to the Wisconsin Department of Agriculture, Trade and Consumer Protection that the breach actually did include Social Security numbers.

Fox and Nesheim each received a copy of the letter. Fox called UnityPoint to get more information about what specific health information had been stolen. She spoke to two representatives, but neither was able to give her further information about the breach. Both representatives told her to "take precautions to protect [her] information." *Id.*, ¶¶ 55, 58. Fox asked if UnityPoint would pay for any "precautions," and UnityPoint said that it would not. After these conversations, Fox subscribed to an online credit monitoring service so that she could be notified of any future identity theft. *Id.*, ¶ 63.

**B. Second data breach**

On May 31, 2018, UnityPoint discovered that hackers had again accessed its employee's email accounts. This time, hackers stole the private information of about 1.4 million patients. Once again, UnityPoint waited two months before it disclosed the breach to the public. On July 30, it sent a letter to affected class members:

> [Stolen information] included your name and one or more of the following information: address, date of birth, Social Security number, driver's license number, medical record number, medical information, treatment information, surgical information, diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information

*Id.*, ¶ 33.

The letter advised recipients to protect themselves against identity theft by monitoring their health information. UnityPoint also offered a complimentary, one-year membership with Experian, which provides identity-theft prevention services. All four plaintiffs received a copy of this letter.

**C. Incidents following the data breaches**

Since the data breaches, plaintiffs have been victims of attempted identity theft and fraud as well as scam phone calls and emails.

In 2018, Fox noticed an increase in autodialed phone calls and spam emails. From April 13 to July 7, she received about 63 autodialed calls to her landline. Several of these calls came from a number identified as "BC Health Clinics," and involved a medical scam. *Id.*, ¶ 52. (Plaintiffs do not provide any further detail about the medical scam.) Fox did not receive any scam medical calls before the data breaches.

Nesheim also received more autodialed calls after the data breaches. These calls were so frequent that Nesheim bought a second phone to use for work. In May or June 2018, Nesheim discovered a suspicious charge on his credit card. He canceled his card and asked his bank to issue a new one. Later, in early July, Nesheim was notified that someone had used his private health information to open a new credit card at a different bank. Nesheim is currently working with that bank to ensure that it did not keep open an account in his name. Had Nesheim known about the data breaches as soon as they occurred, he would have "made a timely and informed decision to take action to mitigate the injury." *Id.*, ¶ 73.

Duckley also received more spam emails and autodialed phone calls after the data breaches. After the second data breach, Duckley became locked out of her pre-existing Experian account due to repeated, unauthorized log-in attempts. When Duckley called Experian to change her password and regain access to the account, Experian told her that the UnityPoint data breach "had undoubtedly been the cause" of the repeated log in attempts. *Id.*, ¶ 76. Had Duckley known about the second data breach as soon as it occurred, she would have "made a more timely and informed decision to take action to mitigate the injury." *Id.*, ¶ 79.

Finally, Kitsis, like the other plaintiffs, received more spam emails and autodialed phone calls after the data breaches. Also, her health information is "extraordinarily sensitive," and the stress caused by the data breach is taking a "significant emotional and physical toll." *Id.*, ¶ 84.

The threat of identity theft is exacerbated by what hackers refer to as "fullz packages." *Id.*, ¶ 66. A fullz package is a dossier that compiles information about a victim from a variety of legal and illegal sources. Hackers can take information obtained in one data breach and cross-reference it against information obtained in other hacks and data breaches. So, for example, if a hacker obtains a victim's Social Security number and health information from UnityPoint, the hacker can combine it with the same victim's Social Security number and phone number from a different data breach. This allows the hacker to compile a full record of information about the individual, which the hacker then sells to others as a package.

The court will discuss additional facts as they become relevant to the analysis.

## ANALYSIS

UnityPoint moves to dismiss plaintiffs' complaint for lack of standing and for failure to state a claim. On all aspects of UnityPoint's motion, the court accepts plaintiffs' well-pleaded factual allegations as true and draws all reasonable inference from those facts in plaintiffs' favor. *Lee v. City of Chicago*, 330 F.3d 456, 459, 468 (7th Cir. 2003). In deciding the jurisdictional issue of standing, the court may consider supporting evidence adduced by the parties. *Id.* at 468. But the court may not consider any evidence from outside the pleadings in deciding the motion to dismiss under Rule 12(b)(6) for failure to state a claim. *Id.* at 459. The question under Rule 12(b)(6) is "simply whether the complaint includes factual allegations that state a plausible claim for relief." *BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015).

## A. Standing

Plaintiffs bear the burden to establish standing to sue in federal court. *Lee*, 330 F.3d at 468. Standing requires (1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). UnityPoint contends that plaintiffs cannot establish the first two elements.

### 1. Injury in fact

"To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted)). "Allegations of *possible* future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (emphasis in original; internal quotations omitted). An injury must be "certainly impending" to constitute an injury in fact. *Id.*

Plaintiffs have alleged several injuries: lost time due to increased spam calls and emails, time spent dealing with fraud attempts, the threat of future identity theft, and money spent mitigating that threat. Any of these allegations would be sufficient to establish standing; even an "identifiable trifle" can constitute an injury in fact. *Craftwood II, Inc. v. Generac Power Sys., Inc.*, 920 F.3d 479, 481 (7th Cir. 2019) (holding that the time lost reading a junk fax before discarding it is a concrete injury) (quoting *United States v. SCRAP*, 412 U.S. 669, 689 n.14 (1973)). And the Court of Appeals for the Seventh Circuit has repeatedly held that injuries like plaintiffs' injuries are sufficient to establish standing in data breach cases.

For example, in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), and *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), hackers stole customer credit-card data from the defendant business. Some customers experienced fraudulent charges on their cards. Their banks reversed the charges, but even with no monetary loss, the customers suffered an injury in the time spent resolving the fraudulent charges. *Lewert*, 819 F.3d at 967. The other customers, who did not experience fraudulent charges, still faced the impending risk of future identity theft. *Id.* at 966. After the data breach, the risk of fraud was more than speculative. "[P]laintiffs 'should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an objectively reasonable likelihood that such injury will occur.'" *Lewert*, 819 F.3d at 966 (quoting *Remijas*, 794 F.3d at 693). The risk of future harm was also evident from the statements of the defendants, who both encouraged their customers to protect themselves from future fraudulent activity. *See Lewert*, 819 F.3d at 967 (defendant acknowledged the risk of fraud in a press release, when it "encouraged consumers to monitor their credit reports"); *Remijas*, 794 F.3d at 694 ("It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014").

UnityPoint argues that under *Remijas* and *Lewert*, the threat of identity theft is not an injury in fact unless plaintiffs allege that hackers "specifically targeted" personal information and that "a certain percentage of that information [was] used to commit fraud." Dkt. 28, at 21. But *Remijas* and *Lewert* did not create a special test for data breach cases. The ultimate question is the same as any case in which a plaintiff alleges a threat of future injury: whether there is an "objectively reasonable likelihood" that an injury will occur. *Remijas*, 794 F.3d at

693 (quoting *Clapper*, 568 U.S. at 410). And in this case, plaintiff have alleged facts sufficient to establish an objectively reasonable likelihood of future identity theft. Personal information, including Social Security numbers, was stolen in the data breaches. The breaches were serious enough that UnityPoint offered identity-theft protection services to the affected customers. And plaintiffs say that thieves used the information to target Fox for a medical scam, open a new credit card in Nesheim's name, and attempt to gain access to Duckley's Experian account. Even if plaintiffs had not already lost time resolving fraud attempts and answering spam calls, the looming threat of fraud would qualify as an injury in fact.

**2. Fairly traceable**

UnityPoint says that hackers may have obtained plaintiffs' information from other sources, and that plaintiffs cannot show that any of their alleged injuries were caused by the UnityPoint data breaches. In the context of standing, the complaint need only allege that "but for" some act or omission of the defendant, the injury would not have occurred. *See, e.g.*, *Lac du Flambeau Band of Lake Superior Chippewa Indians v. Norton*, 422 F.3d 490, 501 (7th Cir. 2005). If a defendant puts forth evidence that challenges standing as a factual matter, then the burden shifts to the plaintiff to "come forward with competent proof that standing exists." *Laurens v. Volvo Cars of N. Am., LLC*, 868 F.3d 622, 626 (7th Cir. 2017) (quoting *Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 444 (7th Cir. 2009)) (internal alterations omitted).

UnityPoint says that it has put forth unrebutted evidence that challenges plaintiffs' allegations of causation: a declaration from UnityPoint's privacy officer that says that no email addresses, passwords, credit card numbers, or "account login information" were stolen in the data breach, Dkt 29, ¶¶ 5–6, and screenshots of Fox's personal website that show that her email address and phone number are publicly available, Dkt. 11. This evidence casts doubt on the

traceability of some of plaintiffs' allegations, namely the increases in spam calls and emails (particularly those received by Fox, who published her contact information) and the fraudulent charge on Nesheim's credit card (because credit card numbers weren't included in the breach). But UnityPoint has not rebutted plaintiffs' allegations that hackers also stole patient names, addresses, Social Security numbers, dates of birth, and medical records. Plaintiffs have plausibly alleged injuries that can be linked to this information. Nesheim says that someone attempted to open a credit card in his name using his personal health information, Dkt. 22, ¶ 71, and Duckley says that someone used information from the data breach to try to log in to her Experian account,[1] *id.*, ¶ 76. Plaintiffs also allege that the information exposed in the first data breach was serious enough that UnityPoint encouraged Fox to "take precautions to protect [her] information." *Id.*, ¶ 55, 58.

Furthermore, UnityPoint's evidence does not challenge plaintiffs' allegations that hackers cross-referenced the data from the breaches and combined it with data from other sources to create "fullz packages." *Id.*, ¶¶ 66–67. UnityPoint argues that the court is not required to accept these allegations as true in a motion under Rule 12(b)(1). But when a defendant does not submit evidence that contradicts a specific allegation, the court accepts that allegation as true—even if the defendant has made factual challenges to other allegations in the complaint. *See Laurens*, 868 F.3d at 626. These allegations plausibly explain why, for example, Fox started getting phone calls related to medical scams after the data breach. The

[1] Experian allows users to log in to its website with either a username and password or with their name, address, Social Security number, and date of birth. *See* Experian login page, available at https://www.experian.com/ncaconline/dispute?intcmp=login_reportnumber.

court can reasonably infer that scammers took the health information from the data breaches and cross-referenced it with Fox's contact information from another source.

In the end, UnityPoint may be correct that some other entity exposed the plaintiffs' private information and is responsible for the injuries listed in the complaint. But that is an issue of causation that will need to be resolved at trial or summary judgment. At this stage plaintiffs have alleged injuries that are fairly traceable to UnityPoint's data breaches.

**B. Failure to state a claim**

Plaintiffs assert 14 claims: (1) negligence, (2) negligence per se, (3) violation of Wisconsin's confidentiality of health records statute, (4) violation of Wisconsin, Illinois, and Iowa's breach notification statutes, (5) invasion of privacy, (6) misrepresentation, (7) breach of contract, (8) breach of the covenant of good faith and fair dealing, (9) violation of the Wisconsin Deceptive Trade Practices Act, (10) violation of the Illinois Uniform Deceptive Trade Practices Act, (11) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, (12) violation of Iowa's consumer fraud statute, (13) unjust enrichment, and (14) declaratory relief.

UnityPoint moves to dismiss all 14 claims under Rule 12(b)(6). The court will evaluate the claims in logical groups, not necessarily the order set forth above.

**1. Choice of law**

Before the court turns to the specific claims, it must consider a preliminary issue: choice of law. The parties agree that Wisconsin law applies to the claims of Fox, Nesheim, and the prospective Wisconsin class members, but they disagree about whether Wisconsin law also applies to the plaintiffs in Illinois and Iowa. Plaintiffs say that Wisconsin law should apply to all plaintiffs. UnityPoint says that Illinois law should apply to Duckley and the prospective

Illinois class members, and that Iowa law should apply to Kitsis and the prospective Iowa class members.

Because Wisconsin is the forum state, the court applies Wisconsin's choice-of-law rules. *Auto–Owners Ins. Co. v. Websolv Computing, Inc.*, 580 F.3d 543, 547 (7th Cir. 2009). Under Wisconsin law, choice-of-law decisions are made on an issue-by-issue basis. *BB Syndication Servs., Inc. v. First Am. Title Ins. Co.*, 780 F.3d 825, 829 (7th Cir. 2015). If the laws of the competing states are the same on a given issue, then the court applies Wisconsin law on that issue. *Id.* But if the states disagree on a given issue, then there are two tests that Wisconsin courts apply to determine which law applies. *Beloit Liquidating Tr. v. Grade*, 2004 WI 39, ¶ 24, 270 Wis. 2d 356, 677 N.W.2d 298. The relationship between the two tests is not entirely clear, but in this case they lead to the same result.

The first test requires the court to consider "whether the contacts of one state to the facts of the case are so obviously limited and minimal that application of that state's law constitutes officious intermeddling." *Drinkwater v. Am. Family Mut. Ins. Co.*, 2006 WI 56, ¶ 41, 290 Wis. 2d 642, 714 N.W.2d 568 (quoting *Beloit Liquidating*, 2004 WI 39, ¶ 24). An alternative version of this test, which applies to contract claims, requires the court to apply Wisconsin law "unless it becomes clear that nonforum contacts are of the greater significance." *Id.*, ¶ 40. Both versions lead to the same conclusion. UnityPoint (an Iowa corporation) provided services to the Illinois and Iowa plaintiffs in their home states. Those plaintiffs, and their claims against UnityPoint, have no connection to the state of Wisconsin, except that they were lumped into this lawsuit with the Wisconsin plaintiffs. But they do have significant connections to the plaintiffs' home states, where the plaintiffs lived, received services, and

allegedly suffered injuries as a result of UnityPoint's actions. The application of Iowa and Illinois law to this case would not constitute any officious intermeddling with Wisconsin.

The second test requires the court to consider five factors to determine which state's laws apply: (1) predictability of results; (2) maintenance of interstate and international order; (3) simplification of the judicial task; (4) advancement of the forum's governmental interests; and (5) application of the better rule of law. *Beloit Liquidating*, 2004 WI 39, ¶ 25. The importance of each factor will vary depending upon the specific facts of the case. *Id*.

In this case, these factors weigh in favor of applying the laws of the nonforum states to the nonforum plaintiffs. The predictability factor deals with the parties' expectations, *Drinkwater*, 2006 WI 56, ¶ 46, and UnityPoint could not have predicted that Wisconsin law would apply to its business with customers in Illinois or Iowa. Likewise, it would interfere with interstate order to supplant the laws of the nonforum states with Wisconsin law. *See Heath v. Zellmer*, 35 Wis. 2d 578, 151 N.W.2d 664, 672 (1967) ("[F]or a state that is only minimally concerned with a transaction or tort to thrust its law upon the parties would be disruptive of the comity between states."). Plaintiffs say that Wisconsin has a governmental interest in applying Wisconsin law, but they do not explain why this interest would extend to UnityPoint customers who do not reside in, or have any connection with, the state of Wisconsin. And it's not clear that any state has a "better" rule of law; this factor requires the court to consider which law "most adequately does justice to the parties and has the greatest likelihood of being applicable with justness in the future." *Beloit Liquidating*, 2004 WI 39, ¶ 31. It's not clear that this is true for any of the states in question. Only one factor weighs in favor of applying Wisconsin law to all plaintiffs: it would be simpler for the court to apply the law of Wisconsin,

because that is the state where the court sits. *See Grade*, 2004 WI 39, ¶ 28. But this factor is outweighed by the other four factors.

Plaintiffs argue that UnityPoint has not identified any conflict between the laws of Wisconsin, Illinois, and Iowa. But as plaintiffs point out (and extensively briefed), all three states recognize different versions of the economic loss doctrine. Dkt. 39, at 22–24. And, as the court will explain below, small variations exist between the states on other issues. Where these variations exist, the court will apply the laws of the nonforum states to the nonforum plaintiffs.

**2. Economic loss doctrine**

UnityPoint contends that in Illinois and Iowa the economic loss doctrine bars plaintiffs' claims for negligence, negligence per se, misrepresentation, and invasion of privacy. (Wisconsin also follows the economic loss doctrine, but the parties agree that Wisconsin's version of the rule does not apply to contracts for services.) The court agrees that the economic loss doctrine applies to the claims for negligence and negligence per se, and it will dismiss those claims for plaintiffs Duckley and Kitsis. The court will dismiss the misrepresentation and invasion-of-privacy claims on other grounds (discussed below), so it need not decide whether the economic loss doctrine applies to them.

The economic loss doctrine bars a plaintiff from using a tort claim to recover purely economic losses arising from a contractual relationship. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (applying Illinois law); *Nebraska Innkeepers, Inc. v. Pittsburgh-Des Moines Corp.*, 345 N.W.2d 124, 128 (Iowa 1984). The rationale is that "tort law affords a remedy for losses occasioned by personal injuries or damage to one's property, but contract law and the Uniform Commercial Code offer the appropriate remedy for economic

losses occasioned by diminished commercial expectations not coupled with injury to person or property." *In re Illinois Bell Switching Station Litig.*, 641 N.E.2d 440, 444 (Illinois 1994). *See also Annett Holdings, Inc. v. Kum & Go, L.C.*, 801 N.W.2d 499, 503 (Iowa 2011) (the rule is intended to avoid the "tortification of contract law"). The economic loss doctrine has been applied to dismiss negligence claims in several data breach cases across the country, including claims brought under Illinois and Iowa law. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1171–76 (D. Minn. 2014) (collecting cases).

Plaintiffs say that Iowa recently abandoned the doctrine when it adopted the Restatement (Third) of Torts. They rely on an unpublished federal district court case that predicts that Iowa courts will stop using the economic loss rule in the future. *See Cont'l W. Ins. Co. v. Cont'l Fire Sprinkler Co.*, No. 4:10-CV-00584-TJS, 2013 WL 12092291, at *1 (S.D. Iowa Mar. 27, 2013). But more recently, the Iowa Supreme Court revisited the economic loss doctrine and described its continued applicability (subject to exceptions that do not apply here). *St. Malachy Roman Catholic Congregation of Geneseo v. Ingram*, 841 N.W.2d 338, 351 (Iowa 2013). Because the Iowa Supreme Court says that it still follows the doctrine, the court will apply it to Kitsis's Iowa claims as well as Duckley's Illinois's claims.

Plaintiffs give three reasons why the doctrine should not apply in this case, but none of them are persuasive. First, plaintiffs say that they have suffered the following non-economic damages: drained phone batteries from an increase in spam calls; lost time; loss in the value of their private health information; and "damages caused by the violation of their privacy rights, attempted and/or actual identity theft and fraud, statutory violations, and being placed at increased risk of identity theft and fraud in the future." Dkt. 39, at 23. But all of these are economic damages because they reflect a pecuniary loss rather than a personal injury or damage

to property. *See Illinois Bell*, 641 N.E.2d at 444; *Nebraska Innkeepers*, 345 N.W.2d at 128. Plaintiffs argue that a phone battery is "damaged" when it loses its charge, but this is a stretch—the only expense associated with a drained phone battery is the money spent recharging it. And claims for inconvenience or lost time fall squarely within the economic loss doctrine. *See e.g. Followell v. Cent. Illinois Pub. Serv. Co.*, 663 N.E.2d 1122, 1124 (Ill. App. Ct. 1996) (lost time due to defective equipment was an economic loss).

Second, plaintiffs cite *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 812 (7th Cir. 2018) (applying Illinois and Missouri law), for the proposition that the economic loss doctrine applies only in cases where the parties have negotiated and established contractual remedies for the underlying harm. But the *Trenton* court did not hold that—it concluded that the doctrine applied even though the plaintiffs in that case did not have any direct contract with the defendant. *Id.* at 814. Instead, both parties had contracts with the same third parties, and because they had the opportunity to negotiate remedies as part of those contracts, the economic loss doctrine barred the introduction of new remedies under a theory of tort. The same logic applies here: the plaintiffs had a contract with UnityPoint for health services, and the parties had an opportunity to include a remedy for data breaches as part of their contract but chose not to.

Third, plaintiffs say that the doctrine does not apply to Duckley or the proposed Illinois class because UnityPoint had a preexisting duty to protect patient health records under federal law. (Although neither party identifies the federal law in question, plaintiffs are presumably referring to the Health Insurance Portability and Accountability Act.) Plaintiffs argue that Illinois has an exception to the economic loss doctrine for duties that exist independent of any contract. *See Congregation of the Passion v. Touche Ross & Co.*, 636 N.E.2d 503, 515 (Illinois

1994). But this exception applies only in professional malpractice cases, such as claims for legal malpractice, in which the defendant is a member of a skilled profession and has a duty of reasonable professional competence. *Michaels Stores*, 830 F. Supp. 2d at 529–30; *see also Trenton*, 887 F.3d at 817 (adopting the *Michael Stores* court's interpretation of Illinois law). It does not apply simply because UnityPoint violated a federal statute.

**3. Negligence under Wisconsin law**

UnityPoint contends that Fox and Nesheim's claims for negligence and negligence per se must be dismissed because plaintiffs have failed to allege "actual damages." But Rule 8 does not create a pleading standard for damages beyond what is necessary to establish standing. *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). "To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available." *Id.* Furthermore, both Fox and Nesheim have alleged measurable, pecuniary damages that they suffered as a result of the data breaches. Fox says that she subscribed to a credit monitoring service to mitigate the risk of identity theft after the first data breach. Dkt. 22, ¶ 63. Nesheim says that he had to buy a second phone to use for work because he received too many spam calls on his personal phone. *Id.*, ¶ 72. This is sufficient at the pleading stage.

**4. Wisconsin confidentiality of health records statute**

Wisconsin Statute § 146.82(1) says that patient health care records may be released only with the informed consent or authorization of the patient, or to persons otherwise designated by the statute. Any person who negligently violates the statute "shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $1,000 and costs and reasonable actual attorney fees." Wis. Stat.

§ 146.84(1)(bm). Plaintiffs Fox and Nesheim say that UnityPoint negligently released their health care records without consent, and that they suffered actual damages through credit-monitoring fees and the cost of buying a new phone to avoid spam calls. That is more than sufficient for Fox and Nesheim to state a claim that they were injured by UnityPoint's violation of the statute.

**5. Invasion of privacy**

The court will dismiss plaintiffs' claims for invasion of privacy because plaintiffs have not alleged that UnityPoint intentionally disclosed their private information. None of the plaintiffs' home states recognize a claim for invasion of privacy for negligent or reckless behavior that results in a third party's disclosure of plaintiffs' private information

The parties focus on Wisconsin law, so the court will start there. In Wisconsin, torts related to the invasion of privacy are codified under Wisconsin Statute § 995.50. Plaintiffs' claims arise under subsection (2)(c), which creates a cause of action for the publication of private information. A claim for publication of private information has four elements: (1) a public disclosure of facts regarding the plaintiff; (2) the facts disclosed are private facts; (3) the private matter made public is one which would be highly offensive to a reasonable person of ordinary sensibilities; and (4) the defendant acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter, or with actual knowledge that none existed. *Pachowitz v. Ledoux*, 2003 WI App 120, ¶ 18, 265 Wis. 2d 631, 666 N.W.2d 88; *Zinda v. Louisiana Pac. Corp.*, 149 Wis.2d 913, 929–30, 440 N.W.2d 548 (1989).

Section 995.50 does not specify whether the first element of this claim requires intentional disclosure by the defendant. But Wisconsin Statute § 893.57 categorizes invasion of privacy as an intentional tort, alongside other intentional torts like assault, battery, and false

imprisonment. And courts that have considered similar claims in other jurisdictions have held that intentional action is required.[2] Section 995.50 is to be "interpreted in accordance with the developing common law of privacy," Wis. Stat. § 995.50(3), so it's likely that Wisconsin courts would come to the same conclusion as these other courts. In contrast, plaintiffs have pointed to no authority (and the court has found none) in which a defendant was held liable under this statute, or a similar statute, for information stolen by a third party.

Plaintiffs nonetheless say that § 995.50 creates a cause of action for negligent or reckless disclosures of information. They make two arguments in support of this interpretation, but neither is persuasive. First, plaintiffs say that the language of the statute grants relief when one's "privacy is unreasonably invaded," Wis. Stat. § 995.50(1), and that the use of the word "unreasonably" creates a negligence standard. But the cited language is from the damages section of the statute, not the liability section. "Unreasonable invasion" is not an element of plaintiffs' claim under subsection (2)(c), nor any of the other claims listed in subsection (2). It is merely shorthand for the invasion of privacy tort.

Second, plaintiffs say that in *Pachowitz*, 2003 WI App 120, ¶ 29, the court held a defendant liable for reckless disclosure of private information. But there was no dispute in that case that the defendant intentionally disclosed the plaintiff's private information. Rather, the issue was whether the defendant acted "recklessly as to whether the information was of legitimate public interest" when he decided to share it with others. *Id.* ¶¶ 28–30.

---

[2] *See, e.g., Elliott-Lewis v. Abbott Labs.*, 378 F. Supp. 3d 67, 71 (D. Mass. 2019); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1288 (N.D. Ala. 2014); *Randolph v. ING Life Ins. and Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009); *see also* 62A Am. Jur. 2d Privacy § 97 ("Because invasion of privacy is an intentional tort, an allegation that a business was negligent in permitting the personal information of a customer to be stolen in a data security breach does not support a claim for invasion of privacy based on the public disclosure of private information.").

Plaintiffs' invasion-of-privacy claims likewise fail under Illinois and Iowa law. In Illinois, there is no common law duty to safeguard personal information from third-party disclosure. *Trenton*, 887 F.3d at 816 (citing *Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 29–29 (Ill. App. Ct. 2010)). Plaintiffs cite *Ainsworth v. Century Supply Co.*, 693 N.E.2d 510, 515 (Ill. App. Ct. 1998), but the cited passage refers to the standard for applying punitive damages under Illinois law. Nothing in that case says that a defendant can be held liable for recklessly allowing a third party to invade one's privacy.

Plaintiffs say that Iowa courts have not decided whether an invasion-of-privacy claim requires the defendant to intentionally publish private information, but that "one would expect Iowa law to follow the same approach as Wisconsin and Illinois."[3] Dkt. 39, at 31. The court agrees with this assessment, but unfortunately for plaintiffs, neither Wisconsin or Illinois allows claims for negligent or reckless publication of private information. So the court will dismiss all the invasion-of-privacy claims.

**6. Fraud and misrepresentation claims**

Plaintiffs assert five claims related to alleged misrepresentations made by UnityPoint: (1) common law misrepresentation, (2) violation of the Wisconsin Deceptive Trade Practices Act, (3) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, (4) violation of the Iowa Consumer Fraud Act, and (5) violation of the Illinois Uniform Deceptive Trade Practices Act. UnityPoint says that all five claims are subject to heightened

[3] UnityPoint cites *Koeppel v. Speirs*, 808 N.W.2d 177, 181 (Iowa 2011), but that case involves a claim for "unreasonable intrusion upon the seclusion of another," which is unrelated to Kitsis's claim that UnityPoint publicized her private information. In Iowa, claims for "unreasonable intrusion" and "unreasonable publicity" are both referred to as claims for "invasion of privacy," and they both "represent an interference with the plaintiff's right to be left alone," but they are otherwise unrelated. *Id.*

pleading standards under Rule 9(b), which requires plaintiffs to plead fraud claims with particularity. Plaintiffs agree that their claims for common law misrepresentation are subject to heightened pleading, but they argue that their statutory claims are subject to ordinary notice pleading under Rule 8.

The court need not decide the pleading standard issue because even under Rule 8's relaxed pleading standard, plaintiffs fail to state any claims related to misrepresentation. The first four claims fail because plaintiffs have not alleged facts showing that they relied on UnityPoint's statements or suffered damages because of them. The claim for violation of the Illinois Uniform Deceptive Trade Practices Act fails because plaintiffs have not alleged facts showing that UnityPoint's misrepresentations are likely to cause future injury.

**a. Common law misrepresentation and consumer fraud statutes**

The court starts with plaintiffs' claim for misrepresentation, together with claims for violation of the Wisconsin Deceptive Trade Practices Act, the Illinois Consumer Fraud and Deceptive Business Practices Act, and the Iowa Consumer Fraud Act. All four claims require plaintiffs to prove either their reliance on UnityPoint's misrepresentations or that they suffered actual damages caused by the misrepresentations.

In Wisconsin, a claim for intentional or negligent misrepresentation requires plaintiffs to prove that (1) the defendant made a representation of fact; (2) that was untrue; and (3) that plaintiffs relied on it to their damage. *Ollerman v. O'Rourke Co., Inc.*, 94 Wis. 2d 17, 25, 288 N.W. 2d 95, 99 (1980). Plaintiffs must also prove reliance to prevail on a misrepresentation claim under Illinois or Iowa law.[4]

[4] *Air Host Cedar Rapids, Inc. v. Cedar Rapids Airport Comm'n,* 464 N.W.2d 450, 453 (Iowa 1990) (a claim for fraudulent misrepresentation requires plaintiffs to prove: (1) a material misrepresentation; (2) made knowingly; (3) with intent to induce the plaintiff to act; (4) upon

A claim under the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18, is similar to a claim for common law misrepresentation, except that plaintiffs do not need to prove reliance. *Novell v. Migliaccio*, 2008 WI 44, ¶ 48, 309 Wis.2d 132, 749 N.W.2d 544. Instead, they must prove that "the representation materially induced (caused) a pecuniary loss to the plaintiff[s]." *Id.*, ¶ 49. Likewise, a claim under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, requires plaintiffs to prove that the misrepresentation caused plaintiffs to suffer "actual pecuniary loss." *Camasta*, 761 F.3d at 739.

Plaintiffs say that the Iowa Consumer Fraud Act, I.C. § 714H, does not require them to prove reliance or damages. But the case they cite, *State ex rel. Miller v. Hydro Mag, Ltd.*, 436 N.W.2d 617, 622 (Iowa 1989), is referring to actions brought by the Iowa attorney general under I.C. § 714.16. Private actions are brought under I.C. § 714H.5, and that statute requires plaintiffs to prove "an ascertainable loss of money or property" caused by the misrepresentation.

With that legal background, the court turns to plaintiffs' allegations. Plaintiffs allege that UnityPoint made two different sets of misrepresentations. First, plaintiffs say that UnityPoint intentionally misrepresented the scope of the breaches by telling customers that the first data breach did not include Social Security numbers and that the second breach did not affect its electronic medical record system. Plaintiffs say that they "believed the statements to be true and relied on them to their detriment," Dkt. 22, ¶ 151, and that had they known about the true extent of the breach, they would have made a "timely and informed decision to

---

which the plaintiff justifiably relies; and (5) damages); *Bd. of Educ. of City of Chicago v. A, C & S, Inc.*, 546 N.E.2d 580, 591 (Illinois 1989) (same). *See also A, C & S, Inc.*, 546 N.E.2d at 591 ("Negligent misrepresentation has essentially the same elements, except that the defendant's mental state is different.").

take action to mitigate the injury," *id.*, ¶¶ 73, 79. But these allegations are conclusory; plaintiffs do not explain how they relied on the statements or would have changed their behavior had they known they were false. And it's not clear what additional steps plaintiffs *could* have taken if UnityPoint had fully informed them. The hackers already had their information. Perhaps some of the plaintiffs would have more quickly signed up for credit-monitoring services, but plaintiffs say that Duckley already had an account with Experian and that this did not stop hackers from allegedly using his data to attempt fraud. A mere statement that plaintiffs could have done something to mitigate their injuries is insufficient to allege reliance or damages.

Second, plaintiffs allege that UnityPoint's privacy policy misrepresented that health care records were "stored in a secure database" that could be accessed by only a few computer technicians. *Id.*, ¶¶ 117, 156. Again, plaintiffs have not alleged facts showing that they relied on these statements or that the statements caused them damage. None of the plaintiffs say that the privacy policy was a factor in their decision to choose UnityPoint as a healthcare provider, or that they were even aware of the policy before the data breach. Plaintiffs alleged facts showing that UnityPoint violated the privacy policy, as discussed below, but that is unrelated to whether the alleged misrepresentations themselves caused damages.

Because the alleged facts fail to show any reliance by plaintiffs, or any link between the alleged misrepresentations and the damages suffered by plaintiffs, the court will dismiss plaintiffs' claims for misrepresentation and violation of the consumer fraud statutes.

**b. Illinois Uniform Deceptive Trade Practices Act**

Duckley contends that UnityPoint's misrepresentations about its security procedures violate the Illinois Uniform Deceptive Trade Practices Act (UDTPA), 815 ILCS 510/2. The UDTPA "was enacted to prohibit unfair competition and was not intended to be a consumer

protection statute." *Chabraja v. Avis Rent A Car Sys., Inc.*, 549 N.E.2d 872, 876 (Ill. App. Ct. 1989). Nonetheless, a consumer may seek injunctive relief under the act if she can show that she is likely to be damaged in the future by the defendant's misleading trade practices. *Popp v. Cash Station, Inc.*, 613 N.E.2d 1150 (Ill. App. Ct. 1992). In most consumer actions, however, the plaintiff is unable to allege facts showing a likelihood of future harm because the harm has already occurred, and because the plaintiff is unlikely to be deceived by defendant's misstatements again in the future. *Reid v. Unilever U.S., Inc.*, 964 F. Supp. 2d 893, 918 (N.D. Ill. 2013).

In this case, Duckley says that UnityPoint has shown a repeated pattern of dishonesty by misrepresenting the scope of its breaches, exaggerating the actions it took in response to the first breach, and continuing to represent that it keeps patient health information in a secure database. In short, UnityPoint "has a history of making empty promises to patients that it will secure their [information] without actually doing so." Dkt. 39, at 27. But even if UnityPoint continues to make similar misrepresentations in the future, Duckley does not explain how this creates a likelihood of future damage to her. She argues that UnityPoint's misrepresentations leave her unaware about the full scope of the data breaches and whether her data is protected from future unauthorized access. But these arguments go to the risk of harm that Duckley faces from the data breaches themselves, not the risk of harm that she faces if UnityPoint continues to misrepresent its protective measures. And because Duckley does not explain how this risk of harm will be abated if the court enters an injunction ordering UnityPoint to stop making misrepresentations, the court will dismiss Duckley's claim under the UDTPA.

### 7. Breach notification statutes

Plaintiffs assert claims for violations of Wisconsin's, Illinois's, and Iowa's data breach notification statutes. The court will dismiss all three claims. The Wisconsin statute does not create a private right of action, and plaintiffs have not alleged facts showing that they suffered damages as a result of UnityPoint's violation of the Illinois and Iowa statutes.

#### a. Wisconsin's notification statue

Under Wisconsin law, a statute provides a private right of action only if there is a clear indication of the legislature's intent to create such a right. *Grube v. Daun*, 210 Wis. 2d 681, 563 N.W.2d 523, 526 (1997). "[T]he general rule is that a statute which does not purport to establish a civil liability, but merely makes provision to secure the safety or welfare of the public as an entity, is not subject to a construction establishing a civil liability." *Id.* at 689 (quoting *McNeill v. Jacobson*, 55 Wis. 2d 254, 198 N.W.2d 611, 614 (1972)). An implied right of action is created only when (1) the language or the form of the statute indicates the legislature's intent to create a private right of action, and (2) the statute establishes private civil liability rather than merely providing for protection of the public. *Miller Aviation v. Milwaukee Cty. Bd. of Supervisors*, 273 F.3d 722, 729 (7th Cir. 2001) (citing *Grube*, 563 N.W.2d at 526).

Wisconsin Statute § 134.98 requires companies that do business in Wisconsin to notify their customers within 45 days of a data breach. But the Wisconsin legislature made clear that violation of the statute does not itself establish civil liability: "Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty." Wis. Stat. § 134.98(4). Plaintiffs concede that, under this language, a "bare procedural violation" of the statute does not impose liability or constitute a breach of duty for a negligence claim. Dkt. 39, at 29. But they argue that the legislature intended to impose

liability when a defendant's violation of the statute is also a violation of a separate, preexisting duty of care. But that would already be a claim for common law negligence, so even in that case, the statute would not create a right of action. Because the legislature has not provided any indication that § 134.98 creates a separate right of action, the court will dismiss plaintiffs' claims under the statute.

**b. Illinois and Iowa data breach statutes**

Unlike the Wisconsin statute, the Illinois data breach statute, 815 ILCS 530/20, clearly creates a private right of action. A violation of the statute constitutes an "unlawful practice" under the Illinois Consumer Fraud Deceptive Business Practices Act. 815 ILCS 530/20. And the Consumer Fraud Act allows consumers to bring private actions when damaged by an unlawful practice. 815 ILCS 505/10a.

The only courts to have interpreted the Iowa breach notification statute, I.C. § 715C.2, have held that it is ambiguous as to whether it creates a private right of action.[5] But plaintiffs contend that, like the Illinois statute, they may bring an action for violation of the Iowa breach notification statute under the Iowa Consumer Fraud Act, I.C. 714H.2. UnityPoint does not respond to plaintiffs' arguments. The court will assume, without deciding, that the Iowa statute works the same way as the Illinois statute, and that a violation of § 715C.2 can give rise to a claim under § 714H.2.

Both Illinois and Iowa require a company to notify its customers of a data breach "without unreasonable delay," 815 ILCS 530/45; I.C. § 715C.2, and plaintiffs allege that UnityPoint violated the statutes by waiting 60 days before notifying affected customers. But,

[5] *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1339 (N.D. Ga. 2019).

as explained above, plaintiffs must allege actual damages to bring a claim under the Illinois or Iowa Consumer Fraud Acts. But just as plaintiffs have failed to allege any damages that were caused by the misrepresentations in the breach notifications, they have failed to allege any damages that were caused by the timing of the notifications. Because plaintiffs do not explain how they would have suffered less damages had UnityPoint notified them sooner, the court will dismiss their claims for violations of the breach notification statutes.

**8. Contract claims**

Plaintiffs assert claims for breach of contract and breach of the covenant of good faith and fair dealing. The court will allow plaintiffs to proceed on both claims.

To state a claim for breach of contract, plaintiffs must allege: "(1) the existence of a valid and enforceable contract; (2) substantial performance by the plaintiff; (3) a breach by the defendant; and (4) resultant damages." *Reger Dev., LLC v. Nat'l City Bank*, 592 F.3d 759, 764 (7th Cir. 2010). Plaintiffs say that the data breaches were caused when UnityPoint breached its privacy policy. UnityPoint says that the privacy policy is not a contract, that it did not breach the policy, and that there are no damages. As already explained above, plaintiffs have adequately alleged that they were damaged by the data breach. So at this point the court need consider only the other two disputed elements.

UnityPoint makes three arguments for why its privacy policy is not an enforceable contract. None are persuasive. First, it says that plaintiffs bought health services, not privacy services, and that there was no separate consideration for the terms of the privacy policy. But plaintiffs do not claim that the privacy policy is a wholly independent contract. Rather, they contend that the policy was incorporated into their contract for health services, and that because they gave consideration for the contract for health services, they do not need to show

independent consideration for the privacy policy. Dkt. 39, at 29 (citing *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2016 WL 754731, at *9 (N.D. Ill. Feb. 23, 2016)). UnityPoint does not respond to this argument. Plaintiffs' allegation that UnityPoint gave each customer a written copy of its privacy policy is sufficient for the court to reasonably infer that the parties intended to incorporate the policy into their contract for health services.

Second, UnityPoint argues that its privacy policy is merely a statement of preexisting legal obligations. The parties agree that one cannot form a contract by simply promising to follow the law, *see, e.g., Johnson v. Maki & Assocs., Inc.*, 682 N.E.2d 1196, 1199 (Ill. App. Ct. 1997), but plaintiffs argue that the privacy policy includes promises that go beyond state and federal regulations. Because UnityPoint does not explain which laws or regulations its privacy policy is meant to enforce, the court declines to dismiss the contract claim on this ground.

Third, UnityPoint argues that the policy is a nonbinding promise because it has a clause that allows UnityPoint to change the terms of the policy and add new provisions. Dkt. 28-1, at 6. UnityPoint cites *First Wisconsin Nat. Bank of Milwaukee v. Oby*, 52 Wis. 2d 1, 188 N.W.2d 454, 457 (1971), which states that a promise is not a contract if "performance depends solely upon [the promisor's] option or discretion, as where the promisor is free to perform or to withdraw from the agreement at will." But unlike the contract at issue in *Oby*, which did not require the parties to perform any actions, the terms of the privacy policy require UnityPoint to "follow the terms of the [policy] currently in effect." Dkt. 28-1, at 6. Furthermore, unlike the contract in *Oby*, which allowed one of the parties to unilaterally cancel the entire contract, the modification clause allows UnityPoint to modify only the terms of the privacy policy. It does not allow UnityPoint to modify or withdraw from the overall contract for medical services. Neither party provides authority that explains whether *Oby* applies to contracts that allow a

party to modify a contract only in part. The parties may raise the issue at summary judgment, but for now, the court concludes that plaintiffs have sufficiently alleged that the policy is a binding contract.

UnityPoint says that even if the policy is binding, plaintiffs have not alleged any breach of the policy. But plaintiffs plausibly allege that UnityPoint breached its promise to store patient information in a "secure database" when it sent patient health information in employee email attachments. And in any event, the allegations in the complaint allow the court to reasonably infer that the data breach occurred because UnityPoint did not follow the procedures laid out in its privacy policy. Plaintiffs have pleaded sufficient facts to survive a motion to dismiss.

As for plaintiffs' claim for breach of the covenant of good faith and fair dealing, UnityPoint says only the court should dismiss it as duplicative of the breach of contract claim. But this claim may be pleaded as an alternative to the breach of contract claim. *See Maryland Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1509 (E.D. Wis. 1996) (finding that despite overlap, common law breach of contract and good faith and fair dealing claims could be pleaded in the alternative). Because that is UnityPoint's only argument for dismissing this claim, the court will allow the claim to proceed.

**9. Unjust enrichment**

As an alternative to the contract claims, plaintiffs assert a claim for unjust enrichment. The elements of this claim are: (1) a benefit conferred by plaintiffs to the defendant; (2) defendant's knowledge of the benefit; and (3) it would be inequitable for defendant to retain the benefit without paying its value. *Admiral Ins. Co. v. Paper Converting Mach. Co.*, 2012 WI 30, 339 Wis. 2d 291, 811 N.W.2d 351.

UnityPoint says that plaintiffs do not state a claim for unjust enrichment because they received the medical services that they paid for. But plaintiffs allege that privacy protection was part of the services that they paid for, and because UnityPoint was negligent in its privacy practices, they did not provide the full benefit of that bargain. These allegations are sufficient at the pleading stage to state a claim.

UnityPoint also says that plaintiffs cannot bring a claim for unjust enrichment because they already allege the existence of a contract for privacy protection. An unjust enrichment claim is unavailable when a contract already establishes rights and remedies. *See Trenton*, 887 F.3d at 819. But plaintiffs are allowed to plead contract and unjust enrichment claims in the alternative. *Cromeens, Holloman, Sibert, Inc. v. AB Volvo*, 349 F.3d 376, 397 (7th Cir. 2003). At this stage, it is too early to tell whether the parties had a valid contract for privacy services. UnityPoint's arguments may be renewed at summary judgment if the evidence supports them.

**10. Declaratory relief**

Plaintiffs final claim is for declaratory relief stating that UnityPoint violated state law, and in particular the Wisconsin Deceptive Trade Practices Act. As part of the declaration, plaintiffs ask the court to order UnityPoint to change its business practices. Although a request for relief is typically not a separate "claim," plaintiffs clarify in their brief in opposition that they are asserting a separate claim for relief under the Declaratory Judgment Act, 28 U.S.C. § 2201, and that they wish to move forward on this claim even if their other claims are dismissed. Dkt. 39, at 35. District courts have discretion when deciding whether to hear claims under the Declaratory Judgment Act. *Wilton v. Seven Falls Co.*, 515 U.S. 277, 288–90 (1995). The court will exercise its discretion to dismiss plaintiffs' claim for declaratory relief in this case.

As explained above, the court is already dismissing plaintiffs' claims under the Wisconsin Deceptive Trade Practices Act (and related statutes in Illinois and Iowa), so it would be odd for the court to require the parties to address whether UnityPoint violated the statute. And if plaintiffs prevail on the claims that are not being dismissed, then they will receive appropriate relief under the applicable state laws. *See* Fed. R. Civ. P. Rule 54(c). There is no need for separate declaratory relief. *See Aslanukov v. Am. Express Travel Related Servs. Co.*, 426 F. Supp. 2d 888, 890-91 (W.D. Wis. 2006) (dismissing claim for declaratory relief when alternative remedies exist).

**C. Leave to amend**

Plaintiffs ask for leave to amend their complaint to cure any deficiencies that lead to claims being dismissed. The court will deny the request because amendment in this case would be futile.

Many of the dismissed claims failed because of legal barriers, not because plaintiffs failed to plead pertinent facts. The Illinois and Iowa negligence claims are barred by the economic loss doctrine, Wisconsin Statute § 134.98 doesn't provide a private right of action, and none of the state recognize claims for reckless invasion of privacy. Likewise, the court exercised its discretion to decline to hear plaintiffs' claims for declaratory relief.

Only the misrepresentation claims and claims for delayed notification of the breach failed due to pleading deficiencies—plaintiffs did not plead actual damages caused by UnityPoint's communications or reliance on those communications. But it's hard to see how plaintiffs can cure these deficiencies. Their alleged injuries all stem from the data breach itself and hackers' potential use of information gathered in the data breach. Whatever statements UnityPoint made about its data security practices or the scope of the data breaches, those

statements had no effect on the degree of harm caused by breaches. The hackers had plaintiffs' information either way.

If plaintiffs can show cause why their amendments would not be futile, then they may file a separate motion for leave to amend. But they will need to point to specific information that was unavailable when they drafted their second amended complaint and explain why it entitles them to a different result.

**D. Conclusion**

The court will dismiss plaintiffs' claims for invasion of privacy, misrepresentation, violation of the consumer fraud statutes, Wis. Stat. § 100.18, 815 ILCS 505/2, I.C. § 714H, violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2, violation of the data breach notification statutes, Wis. Stat. § 134.98(3)(a), 815 ILCS 530/45, I.C. § 715C.2, and declaratory relief. The court will also dismiss the negligence and negligence per se claims for the Illinois and Iowa plaintiffs.

All plaintiffs may proceed on their claims for breach of contract, breach of the covenant of good faith and fair dealing, and unjust enrichment. Fox and Nesheim may also proceed on their claims for violation of the Wisconsin confidentiality of health care records statute, Wis. Stat. §§ 146.81 *et seq*, and for negligence and negligence per se under Wisconsin law.

ORDER

IT IS ORDERED that:

1. Defendant UnityPoint System's motion to dismiss, Dkt. 27, is GRANTED in part:

    a. Plaintiff Danielle Duckley's claims for negligence, negligence per se, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2, and violation of the Illinois data breach notification statute, 815 ILCS 530/45, are DISMISSED.

    b. Plaintiff Shelly Kitsis's claims for negligence, negligence per se, violation of the Iowa Consumer Fraud Act, I.C. § 714H, and violation of the Iowa data breach notification statute, I.C. § 715C.2, are DISMISSED.

    c. Plaintiff Yvonne Fox and Grant Nesheim's claims for violation of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18, and violation of the Wisconsin data breach notification statute, Wis. Stat. § 134.98(3)(a) are DISMISSED.

    d. Plaintiffs' claims for misrepresentation, invasion of privacy, and declaratory relief are DISMISSED.

    e. The motion is denied in all other regards.

2. Plaintiffs' motion to submit supplemental authority, Dkt. 51, is GRANTED.

3. Defendant's motion for leave to respond to the supplemental authority, Dkt. 52, is DENIED.

4. Defendant's motion to submit supplemental authority, Dkt. 53, is GRANTED.

Entered July 24, 2019.

BY THE COURT:

/s/

_____

JAMES D. PETERSON
District Judge